UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/609,809	07/03/2000	Jeffrey Bruce Lotspiech	ARC9-2000-0063-US1	4266

7590 12/16/2004

John L Rogitz
Rogitz & Associates
750 B Street
Suite 3120
San Diego, CA 92101

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 12/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/609,809	LOTSPIECH, JEFFREY BRUCE	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspond nc address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 July 2004* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *6-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *6-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 July 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Response to Arguments

1. In view of the Appeal Brief filed on 7/27/2004, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

2. The amendments will be entered. Applicant cancels claims 1-5. The following claims 6-17 are presented for examination.

Claim Objections

3. **Claim 6** is objected to because of the following informalities: the phrase "in the stream" should read -- in a stream-- . Appropriate correction is required.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

4.1 **Claims 6-7, 11, and 13** are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 6,772,343 to **Shimizu et al**.

4.2 **As per claim 6**, **Shimizu et al** discloses a computer program device, comprising: a computer program storage device including a program of instructions usable by an encryption computer, comprising: chaining of a data block to an adjacent plaintext block *(indicating by column number)* that meets the recitation of logic means for chaining a data block to a plain text version of an adjacent block in a stream to render a chained block, for example (see column 7,

lines 32-35 and 52-55; column 8, lines 42-47); **Shimizu et al** discloses a transformation of the chained block using a key that meets the recitation of logic means for scrambling the chained block using a first round of a cipher to render a scrambled block, for example (see column 8, lines 42-65); and logic means for iterating the means for scrambling and chaining using subsequent rounds of the cipher, for example (see column 8, lines 42-65 and figure 5). A similar process is also performed in another embodiment in figure 7.

As per claim 7, Shimizu et al discloses the limitation of wherein the means for iterating iterates forward and backward through the stream, using successive rounds of the cipher, for example (see column 12, lines 1-47 and figure 7).

As per claim 11, Shimizu et al discloses a method for generating a tamper resistant version of a software program including a stream of data blocks, comprising: providing a cipher defining rounds, for example (see figure 7); iterating through the rounds of the cipher by iterating through respective outer loops of forward plain text chaining followed by backward plain text chaining, for example (see column 12, lines 1-47 and figure 7); and during each forward portion of an outer loop, applying a respective round of the cipher to each block, and during each backward portion of an outer loop , applying a respective round of the cipher to each block, for example (see column 12, lines 1-47 and figure 7).

As per claim 13, Shimizu et al discloses a method for generating a tamper resistant version of a software program including a stream of data blocks, comprising: scrambling a block

using one and only one round of a cipher, for example (see column 8, lines 42-65 and figure 5 and figure 7); then chaining the block to another block to render a chained block, for example (see column 8, lines 42-65 and figure 5); then scrambling the chained block using one and only round of the cipher, for example (see column 8, lines 42-65 and figure 5).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5.1 **Claims 8-10, 12, 14, and 15-17** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,154,541 to **Shimizu et al**.

5.2 **Claims 8, 9, 12, 14, and 16** recite the same inventive concept as claims 6-7, 11, and 13 except for writing the claimed device and method of claims 6, 7, 11, and 13 into algorithm steps. **Shimizu et al** discloses the same inventive concept as discussed previously including the step of determining when to start the backward chaining or ending the loop as explained for example in

column 12. Therefore claims 8, 9, 12, 14, and 16 are rejected on the same rationale as the rejection of claims 6-7, 11, and 13. To one skilled in the art of cryptography, the recited algorithm steps of claims 8, 9, 12, 14, and 16 do not depart in any way from the spirit and scope of the invention disclosed by **Shimizu et al**.

Claim 15 recites the same inventive concept as claim 8 except for using decryption (reversing) the process as opposed to encryption, both encryption and decryption processes are disclosed in **Shimizu et al**. Therefore, claim 15 is rejected on the same rationale as the rejection of claim 8. It is well known in the art that any encryption of a plaintext to a ciphertext can be decrypted with the reverse process to recover the plaintext.

As per claims 10 and 17, Shimizu et al discloses the limitation of wherein a respective round of the cipher is used for each iteration (see column 8, lines 42-65 and figure 5 column 12, lines 1-47 and figure 7).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art discloses the use of block chaining followed by scrambling with variable number of rounds.

US Patents: 6,345,101 Shukla 4,074,066 Ehrsam et al.

6.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

cc

Carl Colin

Patent Examiner

November 18, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100